Proposed new permutation method to secure data in cloud computing

Noor Hussein Nage[1] **and Anwar* Abbas Hattab[2]

[1,2] Computer Science, Faculty of Education, Mustansiriyah University ,Iraq

Abstract. The idea of cloud computing makes it possible to create a shared pool of reconfigurable computing resources (such servers, networks, storage, apps, and services) that can be released and deployed quickly with no administrative effort or communication with service providers. When data is stored in a remote data center, maintaining data security is essential. This can be achieved by encryption. Through the process of encryption, data is changed so that unauthorized users cannot read it.The proposed system uses a new encryption technique that is based on the mathematical properties of the data. The proposed system is more secure than traditional encryption techniques because it utilizes the mathematical properties of the data. It is also more efficient because it doesn't require as much computation as traditional encryption techniques, meaning that less computation is needed.

1 INTRODUCTION

Cloud computing is considered a next-generation technology. It is a web-based technology used to provide premium service[1]. In recent years, cloudcomputing has developed into a new technology and business model. Platformsfor cloud computing offer resources that are simple to access, scalable, reliable, re-configurable, and high performing. Through the Internet, without complex infrastruc- ture management number of clients[2], Means (No direct user management re- quired)[3]. Customers can access a pool of shared computer resources on demand or on a pay-per-use basis using a cloud computing model. Users and organizations can profit from cloud computing in a number of ways, including reduced capital costs and operational costs[4]. Compute, Data as a Service (DaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) are all forms of cloud computing. are the core tenets of cloud computing. This study's goal isto safeguard data in cloud computing[5]. Cloud computing offers a way for cloud datato be stored and retrieved remotely by connecting the cloud app to the internet. By choosing cloud services, customers will be able to save their Meta data in the server for cloud data. Cloud service providers can access or manage the data kept in the cloud data center[6]. Users can access data stored in cloud storage at any time and from any location[7]. The main challenge safety of cloud computing. Data security becomes of utmost importance since cloud data must be sent across the internet. The fundamental data protection practices, such as integrity, accountability, and confiden-tiality, must be maintained. privacy, access control, authentication, and authorization. Using the cloud securely is crucial to safeguarding the cloud computing infrastruc- ture, applications, and data. Different technologies and strategies provide security[8]. Data is kept in the Cloud on a remote, independently managed storage system. You save data at a remote location as opposed to keeping it on your computer's hard disk or another local storage device. The usage of cryptography considerably aids in infor- mation protection. The Economic Times of the Indian Times claims that the act of converting ordinary clear language into unintelligible text and the other way around is what cryptography is all about. Cloud consumers start to worry about the security of their data because of all of these outside managed servers. In order to stop this data leak and other data dangers, information security is necessary. Cryptography is a cru- cial component of information security. To make cloud storage secure[9].

*Corresponding author: noorhussein@uomustansiryah.edu.iq

2 Related Works

In the litera-ture, there are examples successful using Permutation , below are some examples of these studies: In paper [10] The approach that is used to do permutation operations and XOR operations does not require any keys, even if it does use a set of keys that are derived from summation and mean val-ues. in [11]combine permutation and diffusion processes into a whole, namely, simul-taneous permutation and diffusion operation (SPDO).and in [12] The introduced a chaotic color image encryption algorithm using permutation table, S-box and XOR Boolean operation.This paper[13] proposes a novel method for bit permutation in pic-ture encryption, utilizing chaos and a three-dimensional puzzle for further dissemina- tion and confusion. In order to investigate the irreversibility of time series, a novel method called permutation pattern (PP) was proposed in[14]. It may be used to calcu-late the Kullback-Leibler divergence (DKL) and the Jensen-Shannon divergence (DJS). The methods in the previous researches are complex and require time, keys and many treatments,while In this paper, we propose new permutation scheme. So weuse a simple and less complicated method for transaction ciphertext. In this imple- mented method, permutation operation do not require keys, the work depends on a key that represents an attribute of the data, and works to change the locations of the data only. using a set of keys derived from the summed values makes the method sim-ple, fast and less complex.

3 Proposed Approach

In this study, we provide a novel text encryption technique. in cloud computing. In thisapproach, we don't require the user to provide a key for any operation, instead each key is derived from the mathematical properties of the data using a sum operation. In our approach, we divide the text into 256-bit chunks and perform set operations (permuta-tions and shifts) ,as show in figure(1),Each operation will be outlined in more depth below.

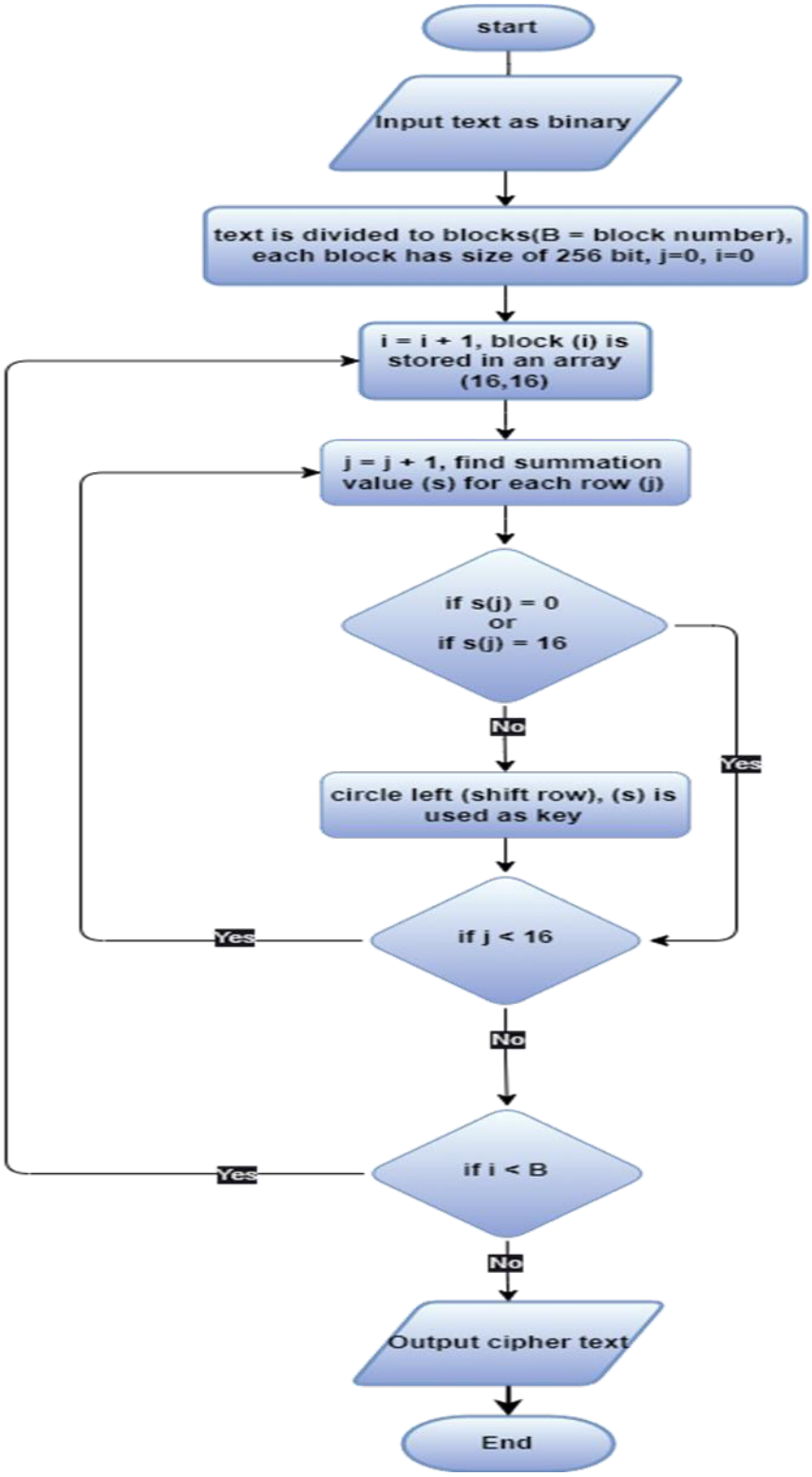

Fig (1). Proposed procedure flowchart

Permutation Operation: Using a block (256 bits) stored in an array of size (16*16),we conduct a sum operation on each row to be utilized as a key for the shift circle for each row in our method. This process creates text diffusion. Example of our permuta- tion operation on an array (5, 5) is shown in Figure 2, and our permutation operation is explained in Algorithm 1.

Instance: let A =

0	1	1	1	1
0	0	0	1	0
0	1	1	0	1
0	0	0	1	1
1	1	1	1	1

1	0	1	1	1
0	0	1	0	0
0	1	0	1	1
0	1	1	0	0
1	1	1	1	1

Sum each row= 4,1,3,2,5

A. Array (A) B. after circular left shift

Fig(2). shows an array with the sum value (5, 5) and an array with a circular left shift.

Algorithm (1) permutation operation

1.Input : text , let x represent text.

2.Output : text after permutation.**Begin** :-

3. Divide x into Blocks, eachblock has 256 bits.

4. Arrange Block into 16x16array.

5. let i represent the current array, starting from array 1.

6. let j represent the current row within array i,starting from row1

7. Calculate Summation for row j in the array i.

8. Let K stand for the summation, which is the permutation operation's key.

9. If K=0 or K=16, then go to step 11

10. circular left shift each row, shift by using (K) as the key.

11. if i = total arrays number, and j = 16, move to step 15

12. j = j + 1

13.if j > 16, make j = 1 and i = i + 1

14.jump to step 7

15.**End**

An example of the permutation process:

Let text x= “NOOR HUSSEN NAGE” , To perform the parsing process on the text, we perform the following steps:

Step1 : To convert the name "NOOR HUSSEIN NAGE" to binary using 8 bits for each letter, you can use the ASCII (American Standard Code for Information Inter- change) representation of each character. Here's the binary representation for each letter:

1. 'N':
ASCII code for 'N' is 78.
In binary, 78 is represented as 1001110.
2. 'O':
ASCII code for 'O' is 79.
In binary, 79 is represented as 1001111.
3. 'O':
ASCII code for 'O' is 79.
In binary, 79 is represented as 1001111.
4. 'R':
ASCII code for 'R' is 82.
In binary, 82 is represented as 1010010.
5. ' ' (Space):
ASCII code for space is 32.
In binary, 32 is represented as 100000.
6. 'H':
ASCII code for 'H' is 72.
In binary, 72 is represented as 1001000.
7. 'U':
ASCII code for 'U' is 85.
In binary, 85 is represented as 1010101.
8. 'S':
ASCII code for 'S' is 83.
In binary, 83 is represented as 1010011.
9. 'S':
ASCII code for 'S' is 83.
In binary, 83 is represented as 1010011.
10. 'E':
ASCII code for 'E' is 69.
In binary, 69 is represented as 1000101.11. 'I':
ASCII code for 'I' is 73.
In binary, 73 is represented as 1001001.

12. 'N':
ASCII code for 'N' is 78.
In binary, 78 is represented as 1001110.
' ' (Space):
ASCII code for space is 32.
In binary, 32 is represented as 100000.15. 'N':
ASCII code for 'N' is 78.
In binary,78 is represented as 1001110.16. 'A':
ASCII code for 'A' is 65.
In binary, 65 is represented as 1000001.17. 'G':
ASCII code for 'G' is 71.
In binary, 71 is represented as 1000111.18. 'E':
ASCII code for 'E' is 69.
In binary, 69 is represented as 1000101.

So, the binary representation of "NOOR HUSSEIN NAGE" using 8 bits for each letter is: 1001110 1001111 1001111 1010010 00100000 1001000 1010101 1010011 1010011
1000101 1001001 1001110 00100000 1001110 1000001 1000111 1000101.

Step2: Divide binary into blocks of 256 bits each and pad with zeros if necessary. To divide the binary representation of "NOOR HUSSEIN NAGE" into blocks of 256 bits each and pad with zeros if necessary, we need to check if the binary string is al- ready a multiple of 256 bits. If not, we'll pad it with zeros to reach the desired length.The binary representation of "NOOR HUSSEIN NAGE" is as follows (spaces added for clarity):
1001110 1001111 1001111 1010010 00100000 1001000 1010101 1010011 1010011
1000101 1001001 1001110 00100000 1001110 1000001 1000111 1000101

Now, let's calculate the length of this binary string:

17 * 8 = 136 bits

Since 136 bits are less than 256 bits, we need to pad it with zeros to reach the desired 256-bitblock size:
1001110 1001111 1001111 1010010 00100000 1001000 1010101 1010011 1010011 1000101 1001001 1001110 00100000 1001110 1000001 1000111 1000101 00000000

Now, the binary representation is divided into blocks of 256 bits each, and zeros have been padded to achieve the desired length

Step 3: Arrange each block in an array of size 16x16.Block 1:
[0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1]
[0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0]
[0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1]
[0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1]
[0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0]
[0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1]
[0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

This represents the 256-bit binary data of "NOOR HUSSEIN NAGE" arranged in a16x16 Each '0' or '1' corresponds to a bit in the binary data.

Step 4: Calculate sum of each row in the block and perform circular left shift based on the sum
Block 1 after circular left shift based on sum:
Row 1: [1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0] (sum = 9)
Row 2: [0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1] (sum = 8)
Row 3: [0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1] (sum = 3)
Row 4: [0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1] (sum = 8)
Row 5: [1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1] (sum = 7)
Row 6: [1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0] (sum = 7)
Row 7: [0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0] (sum = 5)
Row 8: [0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0] (sum = 6)
Row 9: [0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0] (sum = 3)
Row 10: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 11: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 12: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 13: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 14: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 15: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)
Row 16: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] (sum = 0)

Step 5: Convert binary string back to a string

4 Decryption Operation

In the decryption operation, the reverse permutation must be performed using the sum value of each row as the key for the operation and perform shift right circle based on sum value.and the reverse permutation algorithm (2) is described below

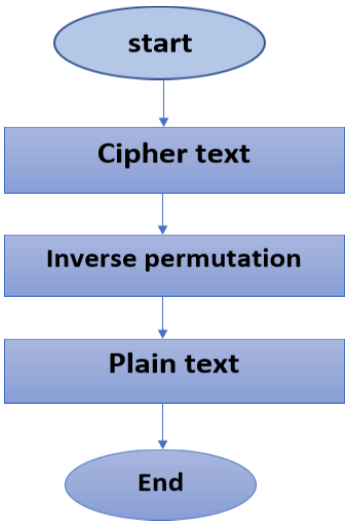

Fig (2) Decryption operation

Algorithm (2) Reverse Permutation

1.Input: cipher text.
2.Output: plain text.Begin:-
3.Divide Binary into Blocks, each block has 256 bits.4.Arrange Block into 16x16 array.
5.let i represent the current array, starting from array1.
6.let j represent the current row within array i,starting from row 1 7.Calculate Summation for row j in the array i.
8. Let K stand for the summation, which is the permutation operation's key.
9.If K=0 or K=16, then go to step 11
10. circular right shift each row, shift by using (-K) as the key.
11. if i = total arrays number, and j = 16, move to step 15
12.j = j + 1
13.if j > 16, make j = 1 and i = i + 1
14.jump to step 7.15.**End**.

-An example of the reverse permutation process:

Step1:After convert string to binary ,and Divide binary into blocks of 256 bits each and pad with zeros if necessary , then Arrange each block in an array of size 16x16 As before, now :

Block 1 after circular shift right based on sum:
Row 1: 0100111001001111 (sum = 9)
Row 2: 0100111101010010 (sum = 8)
Row 3: 0010000001001000 (sum = 3)
Row 4: 0101010101010011 (sum = 8)
Row 5: 0101001101000101 (sum = 7)
Row 6: 0100100101001110 (sum = 7)
Row 7: 0010000001001110 (sum = 5)
Row 8: 0100000101000111 (sum = 6)
Row 9: 0100010100000000 (sum = 3)
Row 10:0000000000000000 (sum = 0)
Row 11:0000000000000000 (sum = 0)
Row 12:0000000000000000 (sum = 0)
Row 13 0000000000000000 (sum = 0)
Row 14 0000000000000000 (sum = 0)
Row 15:0000000000000000 (sum = 0)
Row 16:0000000000000000 (sum = 0)

Convert binary string back to a string :
" NOOR HUSSEIN NAGE"

5 CONCLUSION

In this paper, we present a new permutation-based method for cloud computing text encryption. We present a novel method for generating keys that utilize text attributes as total values (further study may use other attributes). In this strategy, we use a set of keys, but the user does not have to enter the keys. Our suggested encryption technique is easy to use, quick, and might be a viable option for text encryption in cloud computing.

REFERENCES

1. I. No, “Available Online at www.ijarcs.info CLOUD COMPUTING-TECHNOLOGIES,” vol. 9, no. 2, 2018.https://www.researchgate.net/profile/Mohammad-Ilyas-Malik/publication/324863629_CLOUD_COMPUTING-TECHNOLOGIES/links/5af45452aca2720af9c57086/CLOUD-COMPUTING-TECHNOLOGIES.pdf

2. J. Surbiryala and C. Rong, “Cloud computing: History and overview,” *Proc. - 2019 3rd IEEE Int. Conf. Cloud Fog Comput. Technol. Appl. Cloud Summit 2019*, pp. 1–7, 2019, doi: 10.1109/CloudSummit47114.2019.00007. Website link:https://ieeexplore.ieee.org/abstract/document/9045506

3. K. Shaukat and M. U. Hassan, “Cloud computing security using encryption technique,” *Transylvanian Rev.*, vol. 25, no. 12, pp. 74–82, 2017.
Websitelink:https://www.researchgate.net/publication/258201428_Cloud_computing_security_using_encryption_technique

4. N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing ☆,” *Comput. Electr. Eng.*, vol. 71, no. July 2017, pp. 28–42, 2018, doi: 10.1016/j.compeleceng.2018.06.006.
Website link :https://www.sciencedirect.com/science/article/abs/pii/S0045790617320724
5. S. Giri, “Cloud Computing and Data Security Challenges : A Nepal Case,” vol. 67, no. 3,pp. 146–150, 2019.https://www.academia.edu/download/60719932/IJCTTV67I3P128_Cloud_Computing_and_Data_Security_Challenges-_A_Nepal_Case20190927-74024-15q3ep7.pdf
6. I. Zulifqar, S. Anayat, and I. Kharal, “A Review of Data Security Challenges and their Solutions in Cloud Computing,” no. June, pp. 30–38, 2021, doi: 10.5815/ijieeb.2021.03.04.https://www.researchgate.net/profile/SadiaAnayat/publication/352453876_A_Review_of_Data_Security_Challenges_and_their_Solutions_in_Cloud_Computing/links/625e56ff709c5c2adb86809f/A-Review-of-Data-Security-Challenges-and-their-Solutions-in-Cloud-Computing.pdf

7. Rafat Ara | Md. Abdur Rahim | Sujit Roy | Dr. Uzzal Kumar Prodhan, “Cloud Computing Architecture, Services, Deployment Models, Storage, Benefits and Challenges,” *Int. J. Trend Sci. Res. Dev.*, vol. 4, no. 4, pp. 837–842, 2020, [Online]. Available: https://www.researchgate.net/profile/Sujit-Roy9/publication/341788106_Cloud_Computing_Architecture_Services_Deployment_Models_Storage_Benefits_and_Challenges/links/5f5d269ea6fdcc11640ed1f7/Cloud-Computing-Architecture-Services-Deployment-Models-Storage-Benefits-and-Challenges.pdf

8. M. A. Al-Shabi, “A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security,” *Int. J. Sci. Res. Publ.*, vol. 9, no. 3, p. p8779, 2019, doi: 10.29322/ijsrp.9.03.2019.p8779.https://www.researchgate.net/profile/Mohammed-Al Shabi/publication/332176079_A_Survey_on_Symmetric_and_Asymmetric_Cryptography_Algorithms_in_information_Security/links/5d6b8f4da6fdcc547d70434a/A-Survey-on-Symmetric-and-Asymmetric-Cryptography-Algorithms-in-information-Security.pdf
9. S. A. Ahmad, “Computing : A Review,” *2019 15th Int. Conf. Electron. Comput. Comput.*,no. Icecco, pp. 1–6, 2019.https://ieeexplore.ieee.org/abstract/document/9043254/
10. A. A. Hattab, “Proposed Method to Encrypt Images to Mobile Device Based on thePrinciples of Shannon,” vol. 34, no. 6, pp. 820 830,2016.https://www.iasj.net/iasj/download/948cbd58517ffe17
11. L. Liu, Y. Lei, and D. Wang, “A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation,” *IEEE Access*, vol. 8. pp. 27361–27374, 2020. doi:10.1109/ACCESS.2020.2971759.https://ieeexplore.ieee.org/abstract/document/8984280/
12. T. Sajjad and A. Rashid, “A new chaos based color image encryption algorithm using permutation substitution and Boolean operation,” *Multimedia Tools and Applications*. 2020.https://link.springer.com/article/10.1007/s11042-020-08850-5
13. S. F. R. · V. Satpute, “A novel bit per mutation-based image encryption algorithm.”Nonlinear Dynamics.2018.https://link.springer.com/article/10.1007/s11071-018-4600-8
14. J. L. · P. S. · X. Zhang, “Time series irreversibility analysis using Jensen–Shannondivergence calculated by permutation pattern.” Nonlinear Dynamics.2019.https://link.springer.com/article/10.1007/s11071-019-04950-6